D2812 DE (6)

22054
09/980,573

(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 695 01 327 T3** 2005.12.22

(12) Übersetzung der geänderten europäischen Patentschrift

(97) **EP 0 752 143 B2**
(21) Deutsches Aktenzeichen: **695 01 327.0**
(86) PCT-Aktenzeichen: **PCT/US95/03295**
(96) Europäisches Aktenzeichen: **95 914 734.9**
(87) PCT-Veröffentlichungs-Nr.: **WO 95/26013**
(86) PCT-Anmeldetag: **15.03.1995**
(87) Veröffentlichungstag der PCT-Anmeldung: **28.09.1995**
(97) Erstveröffentlichung durch das EPA: **08.01.1997**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **29.12.1997**
(97) Veröffentlichungstag des geänderten Patents beim EPA: **20.07.2005**
(47) Veröffentlichungstag im Patentblatt: **22.12.2005**

(51) Int Cl.[7]: **G07C 9/00**
A61B 5/117

(30) Unionspriorität:
217433 **24.03.1994** **US**

(84) Benannte Vertragsstaaten:
DE, ES, FR, GB, IT, NL

(73) Patentinhaber:
Minnesota Mining and Mfg. Co., Saint Paul, Minn., US

(74) Vertreter:
Vossius & Partner, 81675 München

(72) Erfinder:
OSTEN, David W., Saint Paul, MN 55133-3427, US;
CARIM, Hatim M., Saint Paul, MN 55133-3427, US;
BLAN, Bradford L., Birmingham, AL 35223, US;
ARNESON, Michael R., Westminster, MD 21157, US

(54) Bezeichnung: **Biometrisches Personenauthentifizierungssystem**

Beschreibung

Staatsrechte

[0001] Die vorliegende Erfindung wurde mit Unterstützung der US-Regierung gemäß dem lokalen Untervertrag SO-124465-S und MDA904-93-C4074 entwickelt. Die US-Regierung hat bestimmte Rechte an dieser Erfindung.

Bereich der Erfindung

[0002] Die Erfindung betrifft biometrische Personenauthentifizierungssysteme, durch die Identitäten von Personen authentifiziert werden.

Hintergrund der Erfindung

[0003] Bei Personenerkennungssystemen wird allgemein ein einzelnes hochspezifisches Kennzeichen oder Merkmal ausgewertet, um zu entscheiden, ob ein Ersuchen um Zutritt oder Zugriff berechtigt ist, wobei dieses Verfahren manchmal in Verbindung mit einem anderen Personenauthentifizierungsverfahren verwendet wird.

[0004] In der veröffentlichten Patentanmeldung NL-A-8503290 (Sibum) wird gemäß einer unbeglaubigten Englischübersetzung ein Verfahren zum Identifizieren einer Person durch Erkennen eines gespeicherten Musters, z. B. eines Fingerabdrucks, beschrieben, um einen unberechtigten Zutritt bzw. Zugriff oder eine unberechtigte Benutzung zu verhindern, wobei eine Musteranalyse verwendet wird, bei der die Körperwärme und/oder die Haargröße und -farbe bestimmt werden, um die Verwendung einer gefälschten Kopie des Fingerabdrucks zu verhindern. Daher wird in diesem Dokument ein Verfahren zum Identifizieren einer Person durch die Erfassung mindestens eines inhärent spezifischen biometrischen Parameters der Person, z. B. eines Fingerabdrucks, und Erfassen eines nichtspezifischen biometrischen Parameters, wie beispielsweise der Körperwärme, beschrieben, der während des Authentifizierungsprozesses mit physiologischen Normdaten verglichen werden kann.

[0005] In der veröffentlichten PCT-Patentanmeldung WO 90/08366 (Clayden) wird ein Verfahren zum Identifizieren einer Person durch Überwachen eines oder mehrerer "biometrischer" Parameter, wie beispielsweise des Knochenaufbaus, der Temperatur, des Fingernagelmusters, von Falten in der Handfläche oder den Fingern der Hand, und Vergleichen der überwachten Daten mit gespeicherten Kennzeichen oder Merkmalen beschrieben. Gemäß anderen Verfahren wird Bezug genommen auf Sprache, Handschrift und Registertastatur "-signaturen".

[0006] In der US-A-4896363 (Taylor) wird ein Verfahren zum Analysieren und Vergleichen eines "lebenden" Fingerabdrucks mit einem gespeicherten Datensatz und eine Vorrichtung beschrieben, durch die das Verfahren funktionell umgesetzt wird. In dieser Patentveröffentlichung von Taylor beschriebene herkömmliche Produkte sind beispielsweise eine von Thumbscan Corporation hergestellte Personenzutritts- oder zugriffskontroll-, -überwachungs- oder -sicherungsvorrichtung.

[0007] In der US-A-4869254 und in der US-A-5078136 (beide von Stone et al.) wird ein Verfahren zur nicht-invasiven Messung und Berechnung der Sauerstoffsättigung von Blut im menschlichen Körper unter Übergangsbedingungen und eine Vorrichtung beschrieben, durch die das Verfahren funktionell umgesetzt wird. Die bei Stone et al. beschriebenen herkömmliche Produkte sind allgemein als Pulsoximeter bekannt.

[0008] In der US-A-5103486 (Grippi) wird ein Verfahren zum Abtasten einer Kombination aus einem Fingerabdruck und einer überschriebenen Projektion einer Signatur beschrieben, um ein Individuum zu identifizieren, und die Projektion eines "beliebigen biologischen Merkmals des Benutzers" beansprucht. Ein biologisches Merkmal ist als lebendes Hautgewebe beschrieben.

Zusammenfassung der Erfindung

[0009] Bei keinem der herkömmlichen Authentifizierungs-, Erkennungs- oder Zugangs- bzw. Zugriffssteuerungsverfahren wird das Problem berücksichtigt, daß biometrische Vorrichtungen überlistet werden können, indem ein um biometrische persönliche Authentifizierung ersuchende(s) Individuum bzw. Person das biometrische Muster eines/r autorisierten Individuums bzw. Person vorzeigt, die zum Zeitpunkt der versuchten Authentifizierung oder Erkennung bzw. des versuchten Zutritts oder Zugriffs leistungsunfähig, zergliedert oder verstor-

ben ist.

[0010] D. h., durch keines der herkömmlichen Authentifizierungs-, Erkennungs- oder Zutritts- bzw. Zugriffssicherungssysteme wird die Möglichkeit berücksichtigt, daß biometrische Parameter korreliert sein können oder anderweitig miteinander in Beziehung stehen können, um sicherzustellen, daß eine um eine biometrische Personenauthentifizierung ersuchende Person tatsächlich für die Authentifizierung vorhanden ist. Vorhandene Vorrichtungen können durch eine Person überlistet werden, die von der um Authentifizierung ersuchenden, authentischen Person verschieden ist, indem tatsächlich das biometrische Muster einer um eine biometrische Personenauthentifizierung ersuchenden, autorisierten Person vorgelegt wird.

[0011] Beispielsweise kann eine Fingerabdruckanalyse, bei der nicht berücksichtigt wird, ob der Finger an einem lebenden Menschen befestigt ist, durch elektronische oder photographische Rekonstruktionen des Fingerabdrucks oder durch einen abgetrennten Finger überlistet werden. Andere herkömmlich zur Bestätigung vorgesehene Beweismittel können durch Betrug und Attrappen vorgetäuscht werden.

[0012] Durch die vorliegende Erfindung wird ein bisher nicht berücksichtigtes Problem gelöst, indem ein biometrisches Personenauthentifizierungssystem bereitgestellt wird, bei dem eine Korrelation zwischen einem eindeutigen, inhärent spezifischen biometrischen Parameter mit mindestens einem nichtspezifischen biometrischen Parameter, der während der Authentifizierungszeitdauer meßbar veränderlich ist, in einem physiologischen Toleranzbereich liegt.

[0013] Bei herkömmlichen Verfahren wurden bisher zwei Fehlerarten betrachtet. Die erste Fehlerart ist dadurch gekennzeichnet, daß das Authentifizierungssystem die Authentifizierung eines in Wirklichkeit autorisierten Benutzers fehlerhaft zurückweist. Die zweite Fehlerart ist dadurch gekennzeichnet, daß das Authentifizierungssystem die Authentifizierung eines in Wirklichkeit nicht autorisierten Benutzers fehlerhaft bestätigt. Beide Fehlerarten basieren auf der Genauigkeit bzw. Präzision des auf einem einmaligen, inhärent spezifischen biometrischen Parameter basierenden Authentifizierungsverfahrens. Der Parameter ist möglicherweise zu eng festgelegt (wobei eine Authentifizierung verweigert wird, obwohl sie bestätigt werden sollte), oder zu weit (wobei die Authentifizierung bestätigt wird, obwohl sie verweigert werden sollte). Algemein stehen die beiden Fehlerarten eines Erkennungssystems, bei dem ein einzelner, einmaliger, inhärent spezifischer biometrischer Parameter verwendet wird, invers miteinander in Beziehung. Durch Vermindern der Fehlerrate oder -häufigkeit für eine fehlerhafte Ablehnung oder Verweigerung nimmt die Fehlerrate oder -häufigkeit für eine fehlerhafte Bestätigung zu und umgekehrt. Authentifizierungssysteme, insbesondere Zutritts- oder Zugriffssicherungssysteme, sind mit diesem Konflikt konfrontiert.

[0014] Bei der vorliegenden Erfindung wird eine dritte Fehlerart berücksichtigt und ein bei herkömmlichen Verfahren nicht berücksichtigtes Problem gelöst. Ein unberücksichtigter dritter möglicher Fehler tritt auf, wenn das Authentifizierungssystem die Authentifizierung eines in Wirklichkeit nicht autorisierten Benutzers fehlerhaft bestätigt, der versucht, sich unter Verwendung des Musters eines einmaligen bzw. eindeutigen, inhärent spezifischen biometrischen Parameters eines autorisierten Benutzer Zutritt oder Zugriff zu verschaffen.

[0015] Durch die vorliegende Erfindung werden Fehler der dritten Fehlerart gelöst, indem ein Authentifizierungssystem bereitgestellt wird, das einen eindeutigen, inhärent spezifischen biometrischen Parameter und andere nichtspezifische biometrische Parameter erfaßt, die für die Person nicht eindeutig sein müssen, jedoch mit physiologischen Normdaten vergleichbar und während der Authentifizierungszeitdauer veränderlich sind.

[0016] Durch die vorliegende Erfindung wird das Problem gelöst, daß mindestens zwei biometrische Erkennungsverfahren fehlschlagen oder überlistet werden müssen, um einen nicht autorisierten Benutzer zu authentifizieren.

[0017] "Biometrische Parameter" bezeichnen Größen- und physiologische Kennzeichen oder Merkmale eines einzelnen Menschen. Einige biometrische Parameter (z. B. Fingerabdrücke (einschließlich Daumenabdrücke), Handflächenabdrücke, Porenabdrücke, Sprachmerkmale, Handschrift (einschließlich Signatur) und Netzhaut- oder Retinalstrukturen) sind sowohl eindeutig als auch inhärent spezifisch und relativ leicht kopierbar, reproduzierbar oder modellierbar für einen späteren Vergleich für Authentifizierungszwecke. Eine Fingerabdruckanalyse betrifft die Identifizierung und Messung von Detailpunkten (Verzweigungen und Endpunkte). Eine Porenanalyse betrifft die Identifizierung und Messung von Poren in den Fingerfurchen.

[0018] Andere biometrische Parameter sind für eine Person nichtspezifisch und nicht eindeutig. Nichtspezifische Parameter sind beispielsweise Größenmerkmale (z. B. Knochenstruktur und physische Abmessungen)

und die Hauttemperatur, die sich während der für den Authentifizierungsprozeß erforderlichen Zeitdauer wahrscheinlich nicht verändern, und physiologische Merkmale (z. B. elektrokardiographische (EKG) Signale, Puls und Spektraleigenschaften von menschlichem Gewebe), die sich während der für den Authentifizierungsprozeß erforderlichen Zeitdauer wahrscheinlich meßbar ändern. von diesen beiden Merkmalen sind physiologische Merkmale bedeutungsvoller für eine biometrische Personenauthentifizierung, weil solche physiologischen Merkmale schwerer simulierbar sind, weil solche Meßwerte innerhalb physiologischer Bereiche beobachtbar, zeitveränderlich und durch Kenngrößen, wie beispielsweise EKG und Puls, in einem einzelnen menschlichen Körper synchronisierbar sind.

[0019] Durch einen oder mehrere nichtspezifische biometrische Parameter, die in Kombination mit einem oder mehreren eindeutigen, inhärent spezifischen biometrischen Parametern verwendet werden, wird ein extrem hochpräziser Schutz gegen Überlistung oder Täuschung bereitgestellt, und es ist kein zeitaufwendiger und übermäßiger Meßvorgang für eine Authentifizierung für Zwecke einer Zutritts- oder Zugriffskontrolle für eine Sicherheitsfunktion oder zum Bestätigen der Leistungsfähigkeit zum Ausführen einer Funktion erforderlich. Andere nichtspezifische physiologische Merkmale, wie beispielsweise der Blutalkoholpegel oder die Pegel kontrollierter chemischer Substanzen (z. B. legale Medikamente, die in unzulässigen Mengen oder zu unzulässigen Zeiten verwendet werden, oder illegale Drogen), im Körper könnten verwendet werden, um festzustellen, ob ein ansonsten autorisierter Benutzer sich in einem zulässigen physischen Zustand befindet, in dem ihm der Zugriff auf ein Motorfahrzeug oder Zutritt zu einer anderen Einrichtung oder Apparatur gewährt werden kann.

[0020] Das erfindungsgemäße biometrische Personenauthentifi zierungssystem weist auf:

(a) ein Speichersub- oder -teilsystem zum Speichern eines einmaligen bzw. eindeutigen, inhärent spezifischen biometrischen Parameters mindestens eines/r Individuums bzw. Person einer Art;

(b) ein erstes Erkennungs- oder Erfassungsteilsystem zum Erfassen des einmaligen bzw. eindeutigen, inhärent spezifischen biometrischen Parameters eines/r um persönliche Authentifizierung ersuchenden Individuums bzw. Person;

(c) ein zweites Erkennungs- oder Erfassungsteilsystem zum Erfassen mindestens eines nichtspezifischen Parameters eines physiologischen Merkmals des/der um persönliche Authentifizierung ersuchenden Individuums bzw. Person, das während der Zeitdauer der Authentifizierung meßbar veränderlich ist;

(d) ein erstes Vergleichteilsystem zum Vergleichen des durch das erste Erkennungs- oder Erfassungsteilsystem erfaßten einmaligen bzw. eindeutigen, inhärent spezifischen biometrischen Parameters mit dem im Speicherteilsystem gespeicherten einmaligen bzw. eindeutigen, inhärent spezifischen biometrischen Parameter

(e) ein zweites Vergleichteilsystem zum Vergleichen, ob jeder nichtspezifische biometrische Parameter innerhalb eines zulässigen Bereichs oder Toleranzbereichs mit physiologischen Normdaten für die Art übereinstimmt; und

(f) ein Authentifizierungsuntersystem zum. Bestätigen der Identität eines/r um persönliche Authentifizierung ersuchenden Individuums bzw. Person durch Auswerten der durch das erste und das zweite Vergleichteilsystem durchgeführten Vergleiche, wobei das zweite Erkennungs- oder Erfassungsteilsystem mindestens zwei nichtspezifische biometrische Parameter, die innerhalb eines Toleranzbereichs physiologisch korreliert sind, erfaßt.

[0021] Noch bevorzugter sind die Erfassungprozesse für die beiden nichtspezifischen biometrischen Parameter synchronisiert. Beispiele nichtspezifischer biometrischer Parameter physiologischer Merkmale sind die Blutströmungsgeschwindigkeit, die spektrale Identität von Gewebe, elektrokardiographische Signale, der Puls, die Blutsauerstoffsättigung, Hämatokrit, biochemische Gewebeuntersuchungen, elektrische Plethysmographie, Hautexsudate, mechanische Eigenschaften von Haut, elektrische Eigenschaften von Haut, Transpiration von Gasen, Blutdruck und das differentielle Blutvolumen.

[0022] Am vorteilhaftesten wird beim erfindungsgemäßen biometrischen Personenauthentifizierungssystem eine Fingerabdruckanalyse (die bei der vorliegenden Erfindung eine Daumenabdruckanalyse einschließt) für eine Person in Kombination mit einer Pulsoximetrie und Elektrokardiographie (EKG) der Person verwendet. Durch die Fingerabdruckanalyse wird der eindeutige, inhärent spezifische biometrische Parameter erhalten, während durch die Pulsoximeterdaten und die EKG-Daten der (die) nichtspezifische(n) Parameter erhalten wird/werden, wobei sowohl eine zeitliche Synchronisation zwischen den beiden nichtspezifischen Parametern als auch eine Korrelation zwischen den nichtspezifischen Parametern und dem eindeutigen, inhärent spezifischen biometrischen Parameter gegeben ist. Im einzelnen ist das in Echtzeit gemessene EKG-Signal mit dem durch das Pulsoximeter als Änderung der Blutströmungsgeschwindigkeit in Echtzeit gemessenen Puls synchronisiert.

[0023] Wenn beispielsweise die Fingerabdruckanalyse ergibt, daß der eindeutige, inhärent spezifische biometrische Parameter übereinstimmt, und die Pulsoximeterdaten des Pulses und der prozentualen Sauerstoffsättigung und das EKG-Signal als nichtspezifische biometrische Parameter innerhalb zulässiger Normwerte korrelliert sind und festgestellt wird, daß der durch zwei verschiedene und synchronisierbare Verfahren (elektrisch und optisch) bestimmte Puls synchronisiert ist, wird festgestellt, daß die durch den Fingerabdruck identifizierte Person nicht leistungsunfähig, zergliedert oder verstorben ist, so daß die Authentifizierung der Person erfolgreich ist. Wahlweise kann zusätzlich die Hauttemperatur gemessen werden, um zu bestätigen, daß die um Authentifizierung ersuchende Person lebt.

[0024] Durch die erfindungsgemäße Authentifizierung eines Individuums können verschiedene Funktionen bereitgestellt werden. Nicht als Einschränkung dargestellte Beispiele von für die authentifizierte Person verfügbaren Funktionen sind: Zugriff auf eine Apparatur, Zutritt zu physikalischen Einrichtungen, Erkennung der Person aus verschiedenen Gründen, Bestätigung der Anwesenheit der Person an einem autorisierten Ort oder Verwendung einer autorisierten Apparatur und andere Situationen, bei denen der Zustand einer Person von fern bestimmt oder kontrolliert wird.

[0025] Über die erste Stufe der Authentifizierung einer Person und der Autorisierung des Zutritts zu einer physikalischen Einrichtung oder zur Verwendung einer Apparatur hinaus, kann für eine zweite Stufe einer Zutritts- oder Zugriffskontrolle die geeignete Leistungsfähigkeit bestätigt werden, indem Blutgase oder andere Merkmale oder Kenngrößen gemessen werden, wie beispielsweise der Blutalkoholpegel oder kontrollierte Pegel chemischer Substanzen, durch die die Bedienung einer Apparatur oder eines Geräts, wie beispielsweise eines Massentransportfahrzeugs, durch die Person beeinträchtigt würde.

[0026] Ein Merkmal der vorliegenden Erfindung ist, daß zum Erkennen, zum Vergleichen und zum Feststellen der Authentifizierung inhärent spezifische und nichtspezifische biometrische Parameter gleichzeitig und nichtinvasiv erfaßt werden können.

[0027] Ein anderes Merkmal der vorliegenden Erfindung ist, daß nichtspezifische biometrische Parameter nicht mit der um Personenauthentifizierung ersuchenden Person identifiziert werden müssen.

[0028] Ein Vorteil der vorliegenden Erfindung ist, daß bei um Personenauthentifizierung ersuchenden Personen durch Sicherheitsmaßnahmen, durch die eine fehlerhafte Authentifizierung vermieden wird, mehrere biometrische Parameter verglichen werden.

[0029] Bei einer Ausführungsform der Erfindung ist wahlweise eine Informations- und Dateneingabevorrichtung vorgesehen, um beispielsweise durch Verwendung einer Personenidentifizierungsnummer bzw. eines Personenidentifizierungscodes, eines Photos oder einer anderen Einrichtung bzw. anderer Informationen, die Suche nach gespeicherten Daten des eindeutigen, inhärent spezifischen biometrischen Parameters zu minimieren.

[0030] Bei einer anderen Ausführungsform der Erfindung ist ferner wahlweise eine Vorrichtung zum Lesen und Analysieren codierter und verschlüsselter Informationen vorgesehen, die, anstatt in der Vorrichtung zum Empfangen von Daten des eindeutigen, inhärent spezifischen biometrischen Parameters, auf einem magnetischen oder einem optischen Medium oder einem auf einer Kunststoffkarte gespeicherten Hologramm gespeichert sind, die sich im Besitz der um Authentifizierung ersuchenden Person befindet.

[0031] Bei einer anderen Ausführungsform der Erfindung wird wahlweise eine zusätzliche Authentifizierung unter Verwendung einer Vorrichtung bereitgestellt, durch die mehr als ein eindeutiger, inhärent spezifischer biometrischer Parameter, wie beispielsweise eine geschriebene Signatur oder Unterschrift, eine Retinalstruktur, Spracherkennungsmerkmale oder physische Größen der Person oder von Merkmalen der Person, identifiziert und verglichen werden.

Kurzbeschreibung der Zeichnungen

[0032] Fig. 1 zeigt eine schematische Darstellung einer bevorzugten Ausführungsform der Erfindung;

[0033] Fig. 2a, Fig. 2b und Fig. 2c zeigen Ansichten einer bevorzugten Ausführungsform der Erfindung;

[0034] Fig. 3a, Fig. 3b, und Fig. 3c zeigen Aufrißansichten einer bevorzugten Ausführungsform der Erfindung zum Darstellen von Positionen der Meßvorrichtung;

[0035] Fig. 4 zeigt ein Blockdiagramm der Vorrichtung zum Erkennen des nichtspezifischen biometrischen Parameters elektrokardiographischer Signale;

[0036] Fig. 5 zeigt ein Blockdiagramm der Vorrichtung zum Erkennen des nichtspezifischen biometrischen Parameters der Blutsauerstoffsättigung;

[0037] Fig. 6 zeigt ein Blockdiagramm der Vorrichtung zum Erkennen des nichtspezifischen biometrischen Parameters der Hauttemperatur;

[0038] Fig. 7 zeigt ein Ablaufdiagramm des erfindungsgemäßen Authentifizierungsverfahrens;

[0039] Fig. 8 zeigt ein schematisches elektrisches Schaltungsdiagramm der in Fig. 4 dargestellten Vorrichtung zum Verarbeiten des nichtspezifischen biometrischen Parameters der elektrokardiographischen Signale;

[0040] Fig. 9 zeigt ein schematisches elektrisches Schaltungsdiagramm der in Fig. 5 dargestellten Vorrichtung zum Erzeugen einer gepulsten Betriebsspannung für Rot- und Infrarot(IR)-lampen zum Bestimmen des nichtspezifischen biometrischen Parameters der Blutsauerstoffsättigung;

[0041] Fig. 10 zeigt ein schematisches elektrisches Schaltungsdiagramm der in Fig. 5 dargestellten Vorrichtung zum Verarbeiten der den nichtspezifischen biometrischen Parameter der Blutsauerstoffsättigung anzeigenden Signale; und

[0042] Fig. 11 zeigt ein schematisches elektrisches Schaltungsdiagramm der in Fig. 6 als Blockdiagramm dargestellten Temperaturerfassungsschaltung.

Ausführungsformen der Erfindung

[0043] Fig. 1 zeigt eine schematische Darstellung einer bevorzugten Ausführungsform eines erfindungsgemäßen biometrischen Personenauthentifizierungssystems. Diese Ausführungsform ist eine auf einem Tisch montierte Zutritts- oder Zugriffssicherungseinheit, die die Dateneingabe- und Sensorvorrichtung aufweist. Die Zutritts- oder Zugriffssicherungseinheit ist mit einem geschützten oder gesicherten elektronischen Computersystem verbunden, um die Funktion der Authentifizierung der um Zutritt oder Zugriff ersuchenden Person und die Verwendung des Systems zu ermöglichen.

[0044] Bei dieser Ausführungsform wird ein Teil des Mehrzweckcomputers **2** zum Verarbeiten **6** der den nichtspezifischen biometrischen Parameter anzeigenden Daten und zum Verarbeiten **4** des eindeutigen Fingerabdruckbildes verwendet.

[0045] Eine um Zutritt oder Zugriff ersuchende Person gibt zunächst einen Identifizierungscode ein und ordnet anschließend beide Hände für eine Zeitdauer von etwa zehn Sekunden auf Kontourflächen an, in denen verschiedenartige Sensoren angeordnet sind, bis die Authentifizierung erfolgreich oder erfolglos abgeschlossen ist und vorzugsweise der Zutritt oder Zugriff gewährt oder verweigert wird. Bei der Identifizierungscodeeingabe **8** wird eine Personenidentifizierungsnummer (PIN) eingegeben, oder es kann eine Kennkarte eingeführt und gelesen werden, um über das Zutritts- oder Zugriffssicherungssystem um Zutritt oder Zugriff zu ersuchen. Durch die Verwendung von Personenidentifizierungscodes wird der Suchprozeß eingeengt, der erforderlich ist, um den durch die Vorrichtung erfaßten eindeutigen, inhärent spezifischen biometrischen Parameter mit gespeicherten Daten zu vergleichen. Dies dient dazu, die zum Bestimmen der Personenauthentifizierung erforderlichen Operationen zu beschleunigen. Außerdem kann durch die PIN-Nummer ein zusätzlicher vorläufiger Vergleichspegel für den Authentifizierungsprozeß bereitgestellt werden.

[0046] Elemente eines Authentifizierungssystems sind beispielsweise ein Fingerabdruckbildsensor **10**, durch den Daten für eine Analyse durch Computerlogik- und Speicherfunktionen **4** für eine eindeutige, inhärent spezifische Identifizierung zugeführt werden, und Sensoren **24**, **26** und **28** zum Erfassen nichtspezifischer biometrischer Parameter mit Signalverarbeitungsfunktionen **30** zum Eingeben von Informationen für Analysezwecke an das Computersystem 6 zum Erfassen von Elektrokardiogramm(EKG)-signalen, des Pulses und der Blutsauerstoffsättigung für die nichtspezifische biometrische Validation und der Hauttemperatur für eine weitere wahlweise vorgesehene Validation. Durch diese Kombination von Informationen kann die um Authentifizierung und Zutritt oder Zugriff ersuchende Person eindeutig identifiziert werden, und es kann festgestellt werden, daß die um Authentifizierung ersuchende Person nicht leistungsunfähig, zergliedert oder verstorben ist. D. h. der biologische Zustand der Person, der nichtinvasiv über physiologische Merkmale gemessen wird, die sich wäh-

rend der Authentifizierung zeitlich ändern, wird in Verbindung mit dem eindeutigen, inhärent spezifischen Parameter eines Fingerabdrucks verwendet, um zu bestätigen, daß die Person lebt und innerhalb zulässiger physiologischer Toleranzwerte leistungs- oder arbeitsfähig ist, um sie zu authentifizieren und dadurch den Zutritt oder Zugriff zu gewähren.

[0047] In einer Fingerabdruckerkennungskamera **10** und im System **4** werden bekannte Vorrichtungen, Schaltungen und Programme verwendet. Das Fingerabdruckmuster der Person wird durch die Kamera **10** erfaßt, wenn die Person einen Daumen auf einem Detektorfenster **42** anordnet (in **Fig.** 2 dargestellt und nachstehend beschrieben). Das erfaßte Bild wird aufgenommen und durch eine Bildverarbeitungseinrichtung **12** analysiert und in ein Vektordatenfeld von Fingerabdruckdetails entwickelt, das durch den Vergleicher **14** durch Korrelation des abgetasteten Bildvektordatenfeldes mit einem Datenfeld bestätigt wird, das aus einer durch die PIN-Nummer identifizierten vorgespeicherten Datei **16** ausgewählt wird. Wenn das Bild mit der gespeicherten Information übereinstimmt, wird das Ausgangssignal **18** des Vergleichers **14** eingeschaltet, wodurch der in Fig. 7 dargestellte und nachstehend beschriebene Entscheidungsprozeß veranlaßt wird.

[0048] Fingerabdruckerkennungssysteme, wie beispielsweise die mit dem System **4** zusammenwirkende Kamera **10**, sind kommerziell erhältlich von ThumbScan, Inc., Lombard, Illinois. Ein solches System **4** ist in der US-A-4896363 (Taylor) beschrieben. Alternativ ist die Kamera **10** als Modell FC-11 Fingerprint Capture Station kommerziell erhältlich von Digital Biometrics, Minnetonka, Minnesota. Wenn die Kamera **10** von Digital Biometrics verwendet wird, wird außerdem in Verbindung mit Vergleichssoftware, kommerziell erhältlich von Blitz-Match, Inc., Champaign, Illoinois, ein Rahmenabtaster (frame grabber) IP-8 Image Processing Board, kommerziell erhältlich von Matrox Electronic Systems, LTD., Dorual, Quebec, Kanada, verwendet.

[0049] Das vorgespeicherte Fingerabdruckauswahlmuster kann in einem zugewiesenen ROM-Speicher des Fingerabdruckerkennungssystems **4** oder im Speicher des Computerendgeräts gespeichert sein, auf das die Person über ein Standardtastenfeld zugreifen kann, das mit einem asynchronen Ein-Ausgabeport (I/O-Port) verbunden ist, oder über eine magnetische oder optische Identifizierungskarte, die dem Zutritts- oder Zugriffssicherungsgerät zu dem Zeitpunkt, wenn das Zutritts- oder Zugriffssystem aktiviert wird, dargeboten wird, in das Zutritts- oder Zugriffssicherungssystem eingegeben werden. Die Identifizierungskarte kann die Eingabe der PIN-Nummer unter Verwendung des Tastenfeldes ersetzen oder zusätzlich verwendet werden.

[0050] Die in Fig. 1 dargestellte biometrische Erkennungsschaltung weist auf: biomedizinische (EKG) Elektroden **24** die mit einer Analogsignalverarbeitungseinrichtung **32** verbunden sind, Leuchtdioden(LED)-quellen (eine im sichtbaren bereich (etwa 660 nm), die andere im nahen Infrarot(NIR)-bereich (etwa 910 nm)) und einen Detektor **26**, die mit einer zeit- oder taktgesteuerten Spannungsquelle und einer Signalverarbeitunsgeinrichtung **34** verbunden sind, für die plethysmographischen Signale der Blutpuls-/Sauerstoffüberwachungseinrichtung und einen Temperatursensor **28**, der mit einer Signalverarbeitungseinrichtung und einem Umgebungstemperatursensor **36** verbunden ist.

[0051] Nach einer analogen Verarbeitung werden die Signale über eine Schnittstelle **22** (z. B. eine von Analog Devices, Norwood, Massachusetts erhältliche Karte RIT-815) dem Computersystem **6** digitalisiert für eine Analyse zugeführt. Die digitalisierten Signale werden in der Zentraleinheit (CPU) (z. B. IBM PS/2, erhältlich von IBM Corporation, Armonk, New York) eines Mehrzweck-Computers verarbeitet. Die Sensorsignalverarbeitung **38** folgt einem Logikmuster, das durch Fachleute für die Programmierung des ausgewählten allgemeinen Computers programmiert werden kann. Das Logikmuster umfaßt verschiedene Rechen-, Glättungs- und Vergleichsschritte, wie im Ablaufdiagramm von Fig. 7 dargestellt. Im Speicher **20** sind Toleranzbereiche gespeichert, die bei im Ablaufdiagramm von Fig. 7 definierten Entscheidungsschritten **324**, **328**, **330** und **332** mit den Personendaten verglichen werden.

[0052] **Fig.** 2 zeigt eine auf einem Tisch montierte Ausführungsform einer Zutritts- oder Zugriffssicherungsvorrichtung in drei Ansichten **2a–2c**. Fig. 2a zeigt eine halbfrontale Ansicht **40-A**, Fig. 2b zeigt eine Seitenansicht **40-B** und Fig. 2c zeigt eine Draufsicht **40-C**. Die tischmontierte Zutritts- oder Zugriffssicherungsvorrichtung **60** weist einen Daumen- oder Fingerpasitionierungshohlraum **62**, vorzugsweise mit einer vertieften Platte, zum bequemen Aufnehmen des Daumens oder des Fingers auf, der durch eine vordere Fläche **64** offen ist, die sich in das Innere der Vorrichtung erstreckt, um einen Zugang zu einem Detektorfenster **42** und anderen Sensorelementen zu erhalten, wie nachstehend beschrieben, wobei die Sensoren vor Streulicht geschützt sind. Durch die Position und die Anordnung des Hohlraums **62** kann die rechte und die linke Hand der um Authentifizierung ersuchenden Person auf biomedizinischen Elektroden **44**, **46**, **48** und **50** positioniert werden, so daß der Daumen oder ein Finger einer Hand geeignet auf dem Detektorfenster **42** im Hohlraum ausgerichtet ist. Ein (nicht dargestellter) Schalter kann in der Nähe der Elektroden an der Vorrichtung **60** angeordnet sein,

um einen Abtastvorgang zu aktivieren.

[0053] Das Detektorfenster **42** kann ein Prisma zum Umlenken von Licht sein, das vorzugsweise beschichtet ist, um dem Benutzer ein angenehmes "Gefühl" zu vermitteln, während das Fenster **42** geschützt wird.

[0054] Diese Anordnung ist nur eine unter vielen, durch die die Hände oder andere Körperteile mit den EKG-Elektroden in Kontakt gebracht werden können, während außerdem Positionen für einen ausgewählten Finger oder Zeh auf der Fingerabdruck-Abtasteinrichtung bereitgestellt werden. Beispielsweise könnte der Meßabschnitt im wesentlichen flach sein, wobei das Detektorfenster in der Mitte angeordnet ist und die EKG-Elektroden an beiden Seiten angeordnet sind, so daß ein Zeh oder Finger auf dem Detektorfenster angeordnet werden kann und die EKG-Elektroden mit Abschnitten der Hand oder des Fußes in Kontakt stehen.

[0055] Fig. 2a und Fig. 2c zeigen ein Tastenfeld **54** zum Eingeben einer PIN-Nummer oder einer anderen codierten Information und ein Sichtanzeigefenster **56** zum Ausgeben von Informationen und eines Zustands. Diese Anordnung kann erweitert werden, so daß beispielsweise eine Leseeinrichtung für Identitätskarten (ID-Karten) oder Speichervorrichtungen und akustische Signalwandler für die Eingabe oder Ausgabe von Sprach- oder Tonsignalen vorgesehen sind.

[0056] Diese tischmontierte Ausführungsform eines Zutritts- oder Zugriffssicherungsgeräts ist durch geeignete Elektrokabel (nicht dargestellt) für die Spannungs- Signal und Datenübertragung mit einem Computer verbunden. Es können leicht weitere Geräte in das Zutritts- oder Zugriffssicherungsgerät eingebaut werden, wie beispielsweise ein Mikroprozessor und ein Speicher zum Handhaben oder Steuern der computerbezogenen Logikfunktionen, der Spannungsversorgung und der Ausgabeeinrichtungen, so daß das Ausgangssignal des Geräts ein einfaches Rufsignal zur Verwendung mit einem Relais oder einer anderen Ansprech- oder Antwortvorrichtung sein würde, um der Person Zutritt zur gesicherten Apparatur oder Einrichtung zu ermöglichen, nachdem die Authentifizierung bestätigt wurde.

[0057] Fig. 3a–Fig. 3c zeigen die tischmontierte Ausführungsform des Zutritts- oder Zugriffssicherungsgeräts teilweise im Aufriß, um die Position des Fensters **42** bezüglich einer Federanordnung **90** im Detail darzustellen und darzustellen, daß die Leuchtdioden **92** und **96** dem Photodetektor **98** im wesentlichen diametral gegenüberliegend angeordnet sind. Alternativ können die Leuchtdioden **92** und **96** und der Photodetektor **98** über und unter dem Daumenpositionierungshohlraum angeordnet sein. Ein wahlweise vorgesehener Hauttemperatursensor **80** ist in der Nähe des Fensters **42** in einer Linie mit der Einführachse des Daumenpositionierungshohlraums **62** angeordnet, so daß er in der Nähe der Kontaktstelle des Daumenabdruckbereichs der Hand mit der Haut in Kontakt steht.

[0058] Fig. 4, Fig. 5 und Fig. 6 zeigen Blockdiagramme des Schaltungsaufbaus der Vorrichtungen zum Messen der nichtspezifischen biometrischen Parameter – EKG, Blutsauerstoffgehalt, Puls und Hauttemperatur – wodurch Details des Elektronikblocks **30** der Sensorschnittstelle und der Sensoren **24**, **26** und **28** dargestellt werden.

[0059] Die für die EKG-Signalerfassung verwendeten Sensoren **24** sind Signalelektroden **102** und **104** und eine Erdungselektrode **106**, wie in Fig. 4 dargestellt. Diese Elektroden sind die gleichen wie die Elektroden **46** und **48** bzw. die Erdungselektroden **44** und **50** (die miteinander verbunden sind) von **Fig.** 2, wobei die Erdungselektrode **106** und die erste biomedizinische Elektrode **104** mit der linken Hand und die zweite biomedizinische Elektrode **102** mit der rechten Hand in Kontakt stehen (nicht dargestellt).

[0060] Für die vorliegende Erfindung geeignete biomedizinische Elektroden sind kommerziell erhältlich von Minnesota Mining and Manufacturing Company, St. Paul, Minnesota. Besonders bevorzugte biomedizinische Elektroden sind in der US-A-5012810 (Strand et al.), in der US-A-4524087, in der US-A-4539996, in der US-A-4554924 und in der US-A-4848353 (alle von Engel) und in der US-A-5133356 (Bryan et al.) beschrieben.

[0061] Die Elektroden **102**, **104** und **106** sind so angeordnet, daß ihre leitfähigen Haftmitteloberflächen für einen Kontakt mit Fingern oder Daumen offenliegen. Die Elektroden **102**, **104** und **106** werden periodisch ausgewechselt, wenn die leitfähige Haftmittelkontaktfläche durch Schmutz und trockene Hautschuppen verunreinigt ist. Die Elektroden **102** und **104** sind mit den Eingängen eines Meß- oder Differentialverstärkers **110** verbunden, durch den eine Signalverstärkung mit hoher Eingangsimpedanz erhalten wird, was für eine wirksame Verbindung mit den Elektroden **102** und **104** erforderlich ist. Dem Meßverstärker **110** ist ein Trenn- oder Isolierverstärker **112** nachgeschaltet, um eine elektrische Isolierung zur Person zu erhalten. Der Meßverstärker **110** und der Isolierverstärker **112** werden durch einen isolierten Gleichstrom-Gleichstrom-Wandler

(DC-DC-Wandler) **118** mit Spannung versorgt, durch den ein Schutz durch eine elektrische Isolierung von der Hauptspannungsversorgung erreicht wird.

[0062] Das EKG-Signal wird durch ein Bandpaßfilter **114** verarbeitet, um unerwünschtes Rauschen außerhalb des Frequenzbandes 0,05 Hz bis 30 Hz zu eliminieren, und durch einen Pufferverstärker **116** verstärkt, um Signalpegel des menschlichen Körpers zu kompensieren. Das verarbeitete EKG-Ausgangssignal **126** wird einer Analog/Digital-Schnittstelle **22** zugeführt.

[0063] Fig. 5 zeigt ein Blockdiagramm des Blutsauerstoffsättigungssensors. Der Sensor ist ein bekannter Pulsoximetersensor. Durch die Emissionseinrichtungen und Sensoren dieser Vorrichtung, die im (in **Fig.** 3 dargestellten) Detektorfenster **42** angeordnet sind, wird Licht im nahen Infrarot (NIR) und sichtbares Licht mit verschiedenen Wellenlängen durch menschliches Gewebe des Daumens übertragen und das transmittierte Licht erfaßt. Die Lichtemissionseinrichtungen werden wechselseitig getaktet mit Spannung versorgt, so daß ein Licht ausgeschaltet ist, wenn das andere Licht eingeschaltet ist, wobei die Steuer- oder Schaltfrequenz des Lichts wesentlich größer ist als die menschliche Herzfrequenz und beispielsweise 1500 Hz beträgt.

[0064] Das mit der gleichen Taktfrequenz abgetastete erfaßte Licht ist pulsierendes Licht und steht in direkter Beziehung mit dem normalen Herzpulszyklus. Durch Änderungen der erfaßten Lichtintensität an den Maximum- und Minimumphasen eines bestimmten Pulszyklus wird ein relativer Meßwert des Absorptionsvermögens des Arterienblutes erhalten. Durch Vergleichen der Werte des relativen Absorptionsvermögens bei verschiedenen Wellenlängen (normalerweise etwa 910 nm und 660 nm) kann ein Sauerstoffsättigungswert des Blutes der Person bestimmt werden.

[0065] Die Lichtquelle **140** emittiert Licht mit zwei Wellenlängen. Eine Leuchtdiode (LED) **142**, die Licht mit einer Wellenlänge von 660 nm emittiert, und eine Leuchtdiode (LED) **144**, die Licht mit einer Wellenlänge von 910 nm emittiert, werden durch LED-Treiberquellen **148** und **150** gesteuert. Die Leuchtdioden werden durch einen Taktgenerator **146** getaktet oder zeitgesteuert, der intermittierend ein- und ausgeschaltete Zustände erzeugt, wodurch zwei verschiedene Zustände für die Gesamtlichtquelle bereitgestellt werden: 910 nm-Diode ein/660 nm-Diode aus, dargestellt durch **156**, und 910 nm-Diode aus/660 nm-Diode ein, dargestellt durch **152**.

[0066] Der Detektor **170** wandelt das übertragene Licht durch eine Silicium-Photodiode **172** mit variablem Stromsignal in ein elektrisches Signal um. Das variable Stromsignal wird durch einen Strom-Spannungsverstärker **174** in eine variable Spannung umgewandelt. Die Signalerfassung ist mit der LED-Emissionssteuerung synchronisiert, der während jedem der beiden verschiedenen Zustände übertragene Lichtpegel wird durch Abtast- und Halteschaltungen **182** und **186** erfaßt und gehalten. Jedes übertragene Lichtsignal weist sowohl eine Gleichspannungs-(DC) als auch eine Wechselspannungs-(AC)komponente auf, die für die Berechnung des Blutsauerstoffgehalts und die Verarbeitung in einer Sensorverarbeitungseinrichtung **38** getrennt werden. Das 910 nm-Signal wird verstärkt **190** und gefiltert **192**, um unerwünschte Signale über 10 Hz zu entfernen, und über einen Anschluß **198-D** einer Schnittstelle **22** zugeführt. Die AC-Komponente wird durch ein 0,3 Hz-Hochpaßfilter **194** getrennt, durch einen Verstärker **196** verstärkt und über einen Anschluß **198-A** der Schnittstelle **22** zugeführt.

[0067] Eine parallele Verarbeitung des 660 nm-Signals erfolgt über Kanäle **200**, **202**, **204**, **206** und **208-A** und **208-C**.

[0068] Die Blutsauerstoffmessung dieses Systems ist bekannt und in der US-A-4869254 und in der US-A-5078136 (Stone et al.) beschrieben. Pulsoximeter sind auf die in diesen Patenten beschriebene Weisen kommerziell erhältlich und weisen Leuchtdioden **142** und **144** und einen Detektor **170** auf, die von Nellcor Incorporated, Hayward, Kalifornien, verkauft werden.

[0069] Die Verarbeitung des Pulsoximetersignals wird hierin als Zeitbereichsignalverarbeitung beschrieben. Die Verarbeitung könnte jedoch auch im Frequenzbereich durchgeführt werden, indem das Signal direkt an den Sensoren digitalisiert wird und Digitalsignalverarbeitungsverfahren verwendet werden.

[0070] Wahlweise wird die Hauttemperatur durch einen Festkörpersensor gemessen, dessen Meßbereich so gewählt wird, daß er über den Temperaturbereich des menschlichen Körpers linear ist. Fig. 6 zeigt ein Blockdiagramm der zugeordneten Meßschaltung **250**. Der Hauttemperatursensor **252** wird, um die Person zu schützen, durch den isolierten DC-DC-Wandler **256** mit Spannung versorgt. Die Spannung vom Sensor **252** ist linear abhängig von der Temperatur und wird durch Verstärker **258** und **262** verstärkt und ist von den anderen Schaltungskomponenten getrennt bzw. isoliert. Das Temperatursignal wird gefiltert **264**, um alle Frequenzen über

0,5 Hz zu entfernen, um elektrisches Rauschen zu entfernen, und über einen Anschluß **272** der Schnittstelle **22** zugeführt. Wahlweise kann ein Umgebungstemperatursensor **254** verwendet werden, um Umgebungseinflüsse zu kompensieren, wie im Blockdiagramm **260** dargestellt ist. Das Signal vom wahlweise vorgesehenen Temperatursensor **254** wird durch einen Verstärker **261** verstärkt und über einen Anschluß **268** der Schnittstelle **22** zugeführt.

[0071] Die Erkennung und der Vergleich im biometrischen Personenauthentifizierungssystem basieren anfangs auf der Fingerabdruckerkennung, gefolgt von einer Analyse der biometrischen Sensorsignale für: EKG **126**, NIR-Licht bei 910 nm **198-A** und **198-C** und bei 660 nm **208-A** und **208-C** und die Temperatur **272**. Die Authentifizierungsverarbeitung wird in einem integrierten Logikprogramm in einem Computer **6** unter Verwendung von Programmen durchgeführt, die auf bekannte Weise in WATCOM C-Computercode, Version 9.5 von WATCOM International Corp., Waterloo, Ontario, Kanada, geschrieben sind. Fig. 7 zeigt eine Beschreibung der Erkennungsteilsysteme, der Vergleichteilsysteme und der Authentifizierungsteilsysteme. Alternativ kann die Authentifizierungsverarbeitung in einer für Fachleute bekannten Weise unter Verwendung eines Programms in einem neuronalen Netzwerk durchgeführt werden.

[0072] Die in Fig. 7 dargestellte Authentifizierungsverarbeitung beginnt mit der Tasteneingabe einer PIN-Nummer durch eine um Authentifizierung ersuchende Person oder durch Einführen einer ID-Karte, durch die eine PIN-Identifizierung **300** mitgeteilt wird. Die Person ordnet seine oder ihre Hände in den in den Fig. 2a–Fig. 2c dargestellten Positionen an, und die Fingerabdrücke der Person werden abgetastet **340** und verarbeitet, um einen Referenzvektor **342** zu erhalten. Die geeignete Aufzeichnung **344** wird aus dem Speicher **16** abgerufen und für eine Bestätigung oder Zurückweisung verglichen **346**. Wenn das Vergleichsergebnis eine Zurückweisung oder Verweigerung der Authentifizierung darstellt, ist die Authentifizierung unabhängig vom Ergebnis des Vergleichs der nichtspezifischen biometrischen Parameter fehlgeschlagen. Bei einer bevorzugten Ausführungsform wird der Zutritt oder Zugriff aufgrund der zurückgewiesenen Authentifizierung verweigert.

[0073] Gleichzeitig mit und parallel zu den in den Erkennungs- und Vergleichsverarbeitungsteilsystemen ausgeführten Verarbeitungen zur Fingerabdruckerfassung in Verbindung mit Daten vom Fingerabdruckspeicher werden Schritte zum Erfassen der nichtspezifischen biometrischen Parameter ausgeführt, wie in Fig. 7 dargestellt.

[0074] Biometrische Daten werden über mehrere Abtastvorgänge (etwa 128) des EKG-Signals, der optischen Signale und des wahlweise vorgesehenen Temperatursignals erfaßt und gesammelt **310**, wobei eine Zeitdauer von etwa 3,2 Sekunden und für das EKG-Signal eine Zeitdauer von etwa 0,5 Sekunden erforderlich ist. Die Logikverarbeitung schreitet dann zu einem Schritt zum Analysieren der plethysmographischen, EKG- und Temperatursignale fort, wobei die optischen und die EKG-Signale unter Verwendung einer fließenden 5-Punkte-Mittelwertberechnung **320** geglättet, die Hauptspitzenwerte im EKG-Signal und im optischen 910 nm-Signal ermittelt **322**, die Pulsfrequenz der EKG- und der optischen Signale berechnet **324**, die Minima im 910 nm-NIR-Signal ermittelt **326**, das Sauerstoffsättigungsverhältnis aus dem optischen 660 nm- und dem optischen 910 nm-Signal berechnet **328** und der Mittelwert des Temperatursignals ermittelt und die mittlere Ist-Hauttemperatur berechnet werden **330**.

[0075] Anschließend erfolgt ein Vergleich **332** der gleichzeitig durch das optische 910 nm-Phlethysmographiesignal und das EKG-Signal erhaltenen Pulsfrequenz. Wenn die durch beide Verfahren gemessene Pulsfrequenzen gleichzeitig innerhalb eines Toleranzwertes übereinstimmen, wird die Logikverarbeitung fortgesetzt. Wenn keine gleichzeitige Übereinstimmung innerhalb des Toleranzbereichs vorliegt, wird unabhängig vom Ergebnis des Vergleichs **346** der Fingerabdruckidentifizierung die Authentifizierung zurückgewiesen oder verweigert **352**.

[0076] Wenn die beiden Pulsfrequenzen gleichzeitig innerhalb des Toleranzbereichs liegen, werden physiologische Normwerte der Sauerstoffsättigung, des Pulses und der Temperatur für einen Vergleich **336** mit der berechneten Sauerstoffsättigung **328**, der Pulsfrequenz **324** und der Temperatur **310** abgerufen. Wenn ein zulässiger oder positiver Vergleich **336** vorliegt, wird zusammen mit einem zulässigen oder positiven Fingerabdruckvergleich **336** eine Authentifizierung erhalten oder bestätigt **350**. Wenn kein zulässiger oder positiver Vergleich **336** vorliegt, wird unabhängig vom Ergebnis des Fingerabdruckvergleichs **346** die Authentifizierung zurückgewiesen oder verweigert **354**. Gegenwärtig bevorzugt gewährt das Authentifizierungsteilsystem dann den Zutritt zu einer Apparatur oder zu Einrichtungen.

[0077] Fig. 8 zeigt ein Schaltungsdiagramm der in Fig. 4 als Blockdiagramm dargestellten EKG-Schaltung im Detail. Tabelle 1 zeigt eine Auflistung von in dieser Schaltung verwendeten Bauteilen und Vorrichtungen.

Tabelle 1
Bauteile

B1, B2	NE2H-Lampe
C1, C2	500 pF
C3	200 pF
C4, C5, C8	1 µF
C6, C7	10 µF
C9, C10, C11, C12, C13, C14	0,56 µF
R2, R1	300 kΩ
R3, R4, R7	50 kΩ
R5, R6	5 MΩ
R8, R9, R10, R11, R12	20 kΩ
R13, R34	2,2 kΩ
R14	30 kΩ
R16	1 MΩ
R17	4,75 kΩ
R18	47 kΩ
R19, R20, R21, R22, R23, R24	10 kΩ
R35	100 Ω
R36, R37	22 kΩ
R64	1 kΩ

Vorrichtungen

U1, U3, U4 Operationsverstärker: National Semiconductor Santa Clara, Kalifornien	LF444CN
U2 Hochspannungs-Trennverstärker Burr-Brown Tucson, Arizona	ISO107A
D1, D2, D3, D4	1N4148
D6, D7 Diode: National Semiconductor Santa Clara, Kalifornien	1N914

[0078] Fig. 9 zeigt das detaillierte Schaltungsdiagramm einer in Fig. 5 als Blockdiagramm **140** dargestellten Blutoximeter-Lichtleistungsschaltung. Tabelle 2 zeigt eine Aufistung der in dieser Schaltung verwendeten Bauteile und Vorrichtungen.

Tabelle 2
Bauteile

C21	1,0 µF
C19	0,01 µF
C20	4700 pF
C22	4,9 µF
C25	5,3 µF
C32	5,4 µF
C40	1 µF
R40	1 MΩ
R41	47 kΩ
R46, R49, R50	10 kΩ
R38	1 kΩ
R39	200 kΩ
R45, R43	4,7 kΩ
R47, R48	470 Ω
R42, R44, R51	10 Ω

Vorrichtungen	
U9 Takt-/Zeitgeber: National Semiconductor Santa Clara, Kalifornien	LM555CN-1500 Hz
U10 Analogschalter: Siliconix Santa Clara, Kalifornien	DG211
D5 Diode: National Semiconductor Santa Clara, Kalifornien	1N4148
Q1, Q2	2N4403
Q3, Q4, Q5, Q6 Transistor: National Semiconductor Santa Clara, Kalifornien	2N4401
U4 Operationsverstärker: National Semiconductor Santa Clara, Kalifornien	LF444C4
U14 Torschaltung: National Semiconductor Santa Clara, Kalifornien	74HCT04

[0079] Fig. 10 zeigt ein detailliertes Schaltungsdiagramm der in Fig. 5 als Blockdiagramm **170** dargestellten Blutoximeter-Leseschaltung. Tabelle 3 zeigt eine Auflistung der in dieser Schaltung verwendeten Bauteile und Vorrichtungen.

Tabelle 3
Bauteile

C42, C43	0,1 µF
C44, C45, C47, C48, C49 C50, C52, C53, C56	0,47 µF
C57	10 pF
R15	10 MΩ
R54, R55, R56, R57 R62, R63, R64, R65	25 kΩ
R52, R53	560 Ω
R66, R58	1,0 MΩ
R67, R59	5 kΩ
R60, R68	330 kΩ

Vorrichtungen	
U6, U7, U8 Operationsverstärker: National Semiconductor Santa Clara, Kalifornien	LF444CN
U12, U11 Halteverstärker: National Semiconductor Santa Clara, Kalifornien	LF398

[0080] Fig. 11 zeigt ein detailliertes Schaltungsdiagramm der in Fig. 6 als Blockdiagramme **250** und **260** dargestellten Temperatursensorschaltung. Tabelle 4 zeigt eine Auflistung der in dieser Schaltung verwendeten Bauteile und Vorrichtungen.

Tabelle 4
Bauteile

C15	1,0 µF
R30	475 kΩ
R26, R29, R32, R33	4,75 kΩ
R28, R25	100 kΩ
R27	23,5 kΩ
R31	240 kΩ

Vorrichtungen

U4 Operationsverstärker: National Semiconductor Santa Clara, Kalifornien LF444CN
DS1 Murata Manufacturing Co., Ltd. Kyoto, Japan E10051
T2 National Semiconductor Santa Clara, Kalifornien LM34

Patentansprüche

1. Biometrisches Personenauthentifizierungssystem mit:
(a) einem Speicherteilsystem zum Speichern eines einmaligen, inhärent spezifischen biometrischen Parameters mindestens eines Individuums einer Art;
(b) einem ersten Nachweisteilsystem zum Nachweis des einmaligen, inhärent spezifischen biometrischen Parameters eines um persönliche Authentifizierung ersuchenden Individuums;
(c) einem zweiten Nachweisteilsystem zum Nachweis mindestens eines nichtspezifischen biometrischen Parameters eines physiologischen Merkmals des um persönliche Authentifizierung ersuchenden Individuums, das während der Zeitdauer der Authentifizierung meßbar veränderlich ist;
(d) einem ersten Vergleichsteilsystem zum Vergleichen des durch das erste Nachweisteilsystem nachgewiesenen einmaligen, inhärent spezifischen biometrischen Parameters mit dem im Speicherteilsystem gespeicherten einmaligen, inhärent spezifischen biometrischen Parameter;
(e) einem zweiten Vergleichsteilsystem zum Vergleichen jedes nichtspezifischen biometrischen Parameters mit physiologischen Normdaten für die Art; und
(f) einem Authentifizierungsteilsystem zum Bestätigen der Identität des um persönliche Authentifizierung ersuchenden Individuums durch Auswerten der durch das erste und das zweite Vergleichsteilsystem erhaltenen Vergleichsergebnisse,
wobei mindestens zwei unterschiedliche nichtspezifische biometrische Parameter durch das zweite Nachweisteilsystem nachgewiesen und durch das zweite Vergleichsteilsystem verglichen werden, wobei innerhalb eines Toleranzbereichs eine physiologische Korrelation zwischen den beiden unterschiedlichen nichtspezifischen biometrischen Parametern besteht.

2. System nach Anspruch 1, wobei das Speicherteilsystem verwendet wird, um die Datenbanksuche zu begrenzen, indem eine Personenidentifizierungs-Codenummer verarbeitet wird, oder wobei das Speicherteilsystem auf einer im Besitz eines Individuums befindlichen Karte vorhanden ist oder wobei das Speicherteilsystem auch Daten des einmaligen, inhärent biometrischen Erfassungssystems enthält.

3. System nach Anspruch 1 oder 2, wobei der nichtspezifische biometrische Parameter aus der Pulsfrequenz, elektrokardiographischen Signalen, Spektralmerkmalen des menschlichen Gewebes, der prozentualen Sauerstoffaufnahme des Blutes, der Perfusion, dem Hämatokrit, biochemischen Gewebeuntersuchungen, der elektrischen Plethysmographie, Hautexsudaten, mechanischen Eigenschaften der Haut, Gastransporteigenschaften, dem Blutdruck, differentiellen Blutvolumina und Kombinationen davon ausgewählt wird.

4. System nach einem der Ansprüche 1 bis 3, wobei die nichtspezifischen biometrischen Parameter außerdem die Hauttemperatur umfassen.

5. System nach einem der Ansprüche 1 bis 4, wobei der einmalige, inhärent spezifische biometrische Parameter aus einem Fingerabdruck, Porenabdruck, Handflächenahdruck, Stimmabdruck und der Netzhautstruktur ausgewählt wird.

6. System nach einem der Ansprüche 1 bis 5, das ferner ein Zutritts- oder Zugriffsteilsystem zum Messen des Alkoholgehalts oder des Gehalts einer kontrollierten chemischen Substanz im Blut eines erfolgreich authentifizierten Individuums aufweist.

7. Vorrichtung mit dem System nach einem der Ansprüche 1 bis 6 zur Steuerung des Zutritts oder Zugriffs zu einer Einrichtung durch Authentifizieren eines Individuums unter Verwendung des Systems nach einem der Ansprüche 1 bis 6.

8. Vorrichtung nach Anspruch 7, wobei das System außerdem ein Zutritts- oder Zugriffsteilsystem zum Messen des Alkoholgehalts oder des Gehalts einer kontrollierten chemischen Substanz im Blut eines erfolgreich authentifizierten Individuums aufweist und wobei der Zutritt oder Zugriff zu der Einrichtung durch das Zutritts- oder Zugriffsteilsystem gesteuert wird, nachdem ein Individuum erfolgreich authentifiziert ist.

9. Verfahren zum Authentifizieren eines Individuums unter Verwendung des Systems nach einem der Ansprüche 1 bis 6, mit den Schritten:
(a) Anordnen beider Hände eines Individuums in einer Vorrichtung, die das System nach einem der Ansprüche 1 bis 6 aufweist, das einen einmaligen, inhärent spezifischen biometrischen Parameter und gleichzeitig mindestens einen nichtspezifischen biometrischen Parameter eines physiologischen Merkmals erkennt, das während der Zeitdauer der Authentifizierung meßbar veränderlich ist; und
(b) Vergleichen der durch das System nach einem der Ansprüche 1 bis 6 nachgewiesenen biometrischen Parameter, um die Identität des um persönliche Authentifizierung ersuchenden Individuums zu bestätigen.

Es folgen 10 Blatt Zeichnungen

Anhängende Zeichnungen

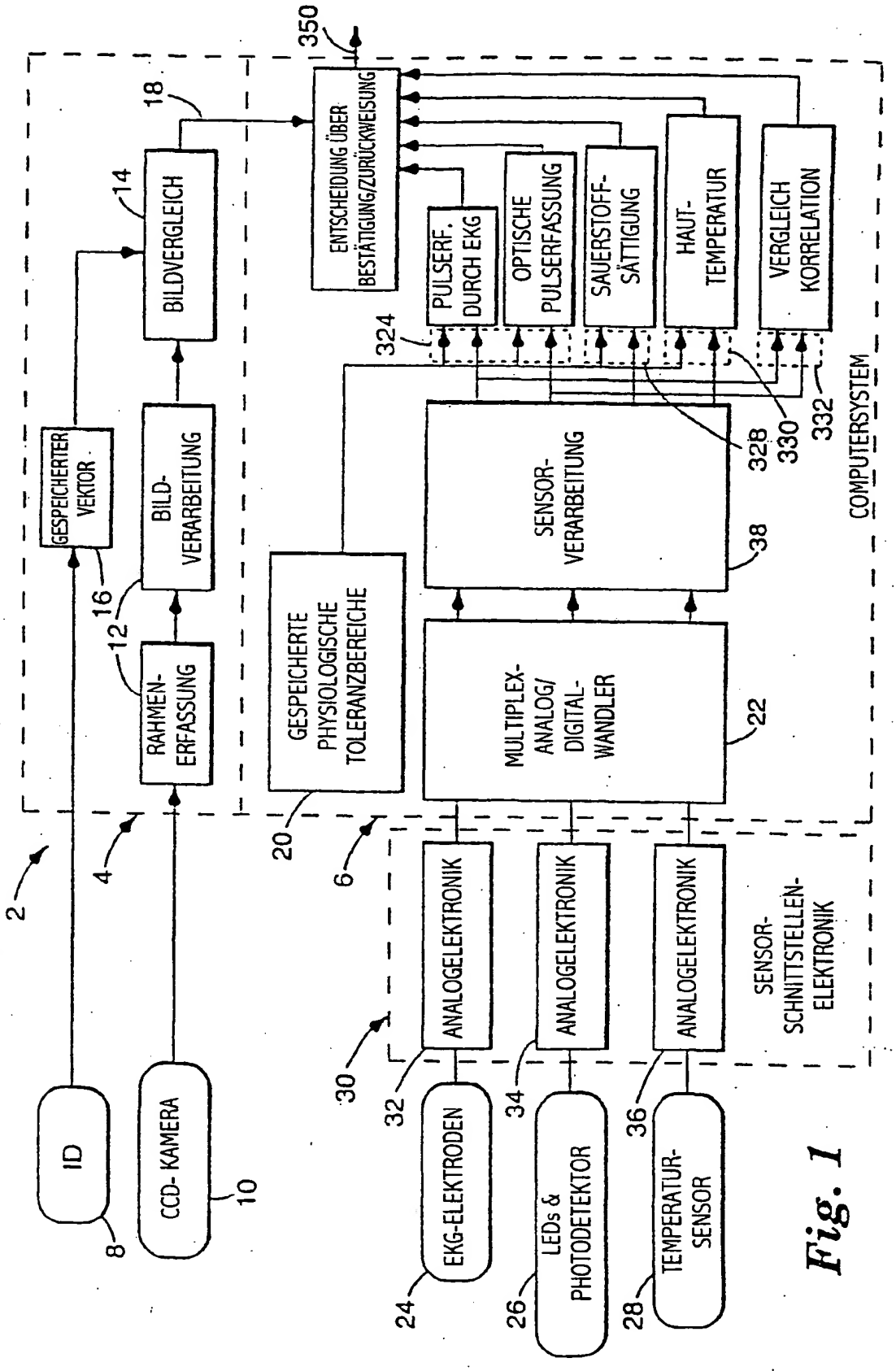


Fig. 1

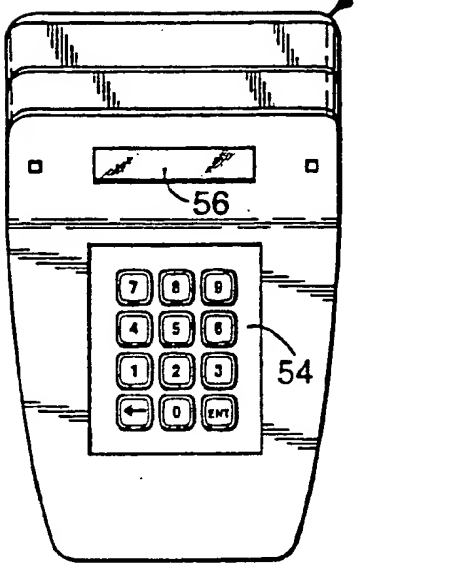


Fig. 2c

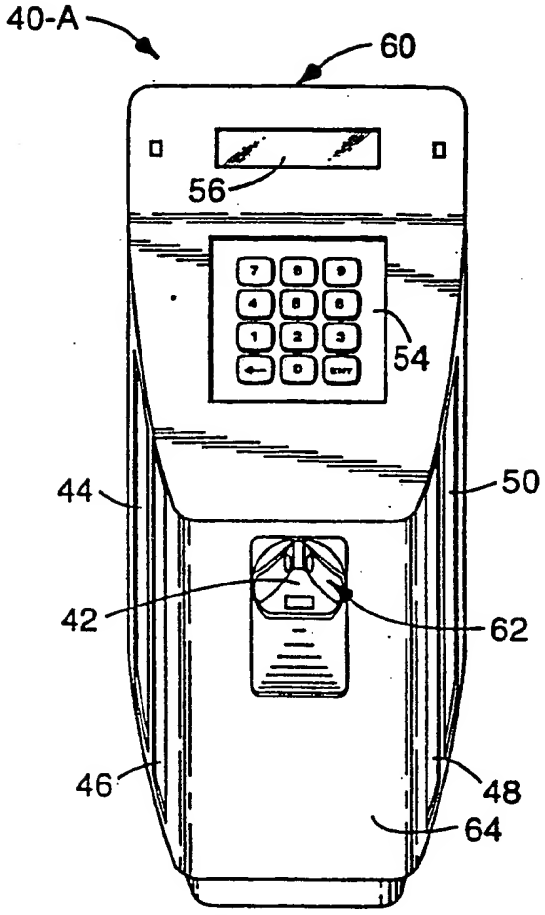


Fig. 2a

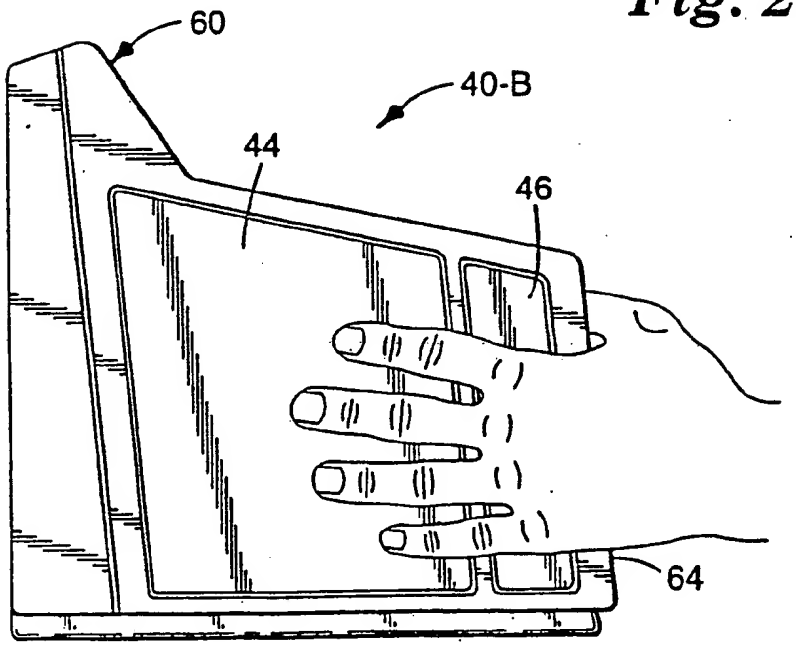


Fig. 2b

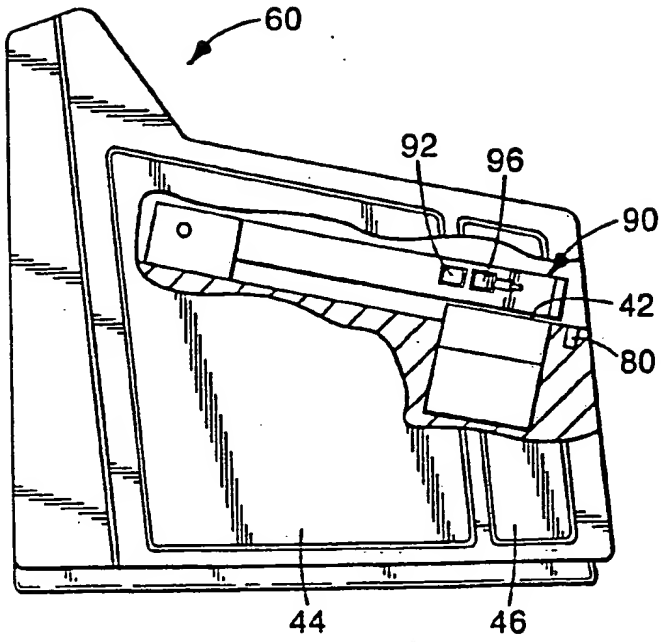


Fig. 3a

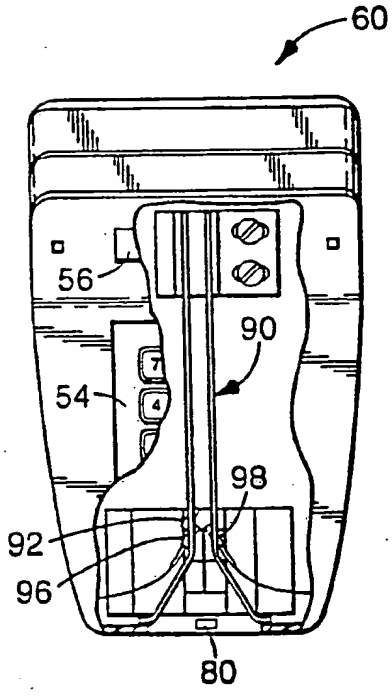


Fig. 3b

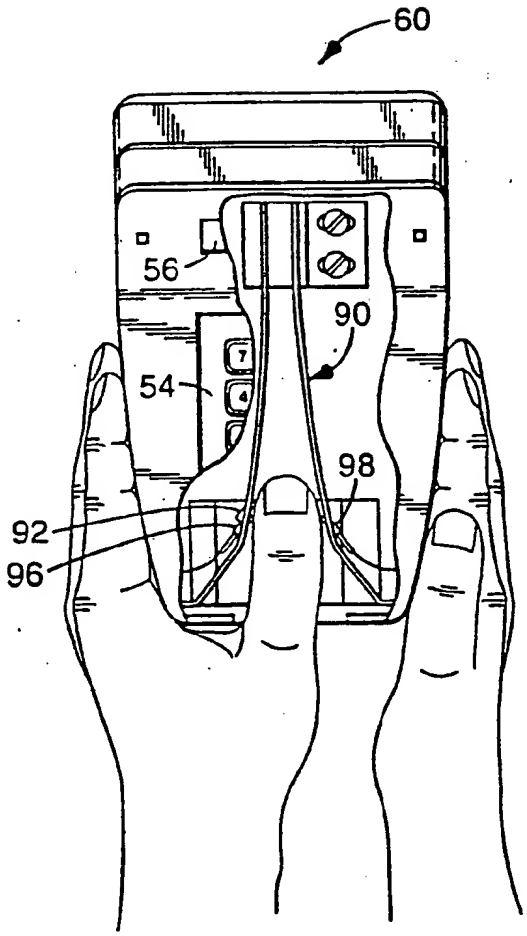


Fig. 3c

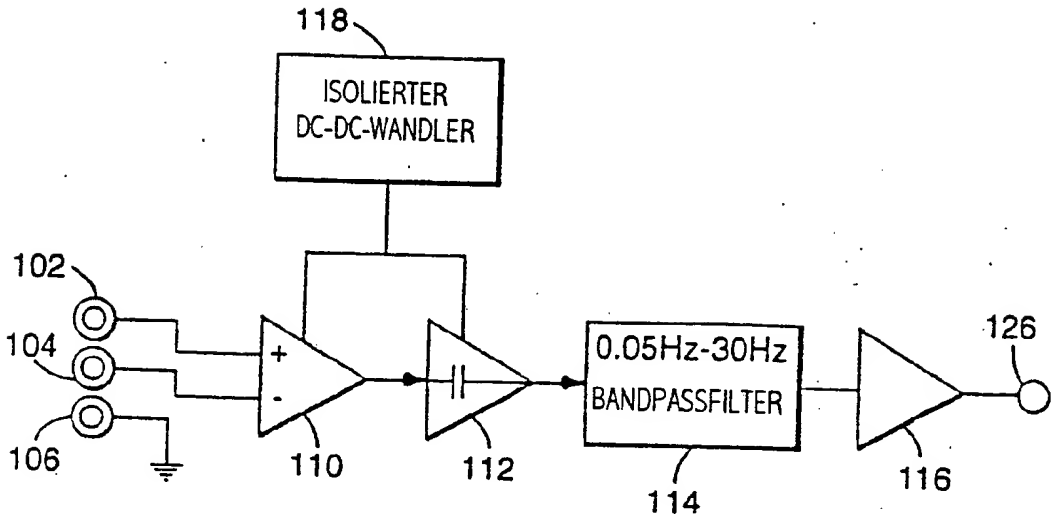

118
ISOLIERTER
DC-DC-WANDLER
102
104
106
+
-
110
112
0.05Hz-30Hz
BANDPASSFILTER
114
116
126

Fig. 4

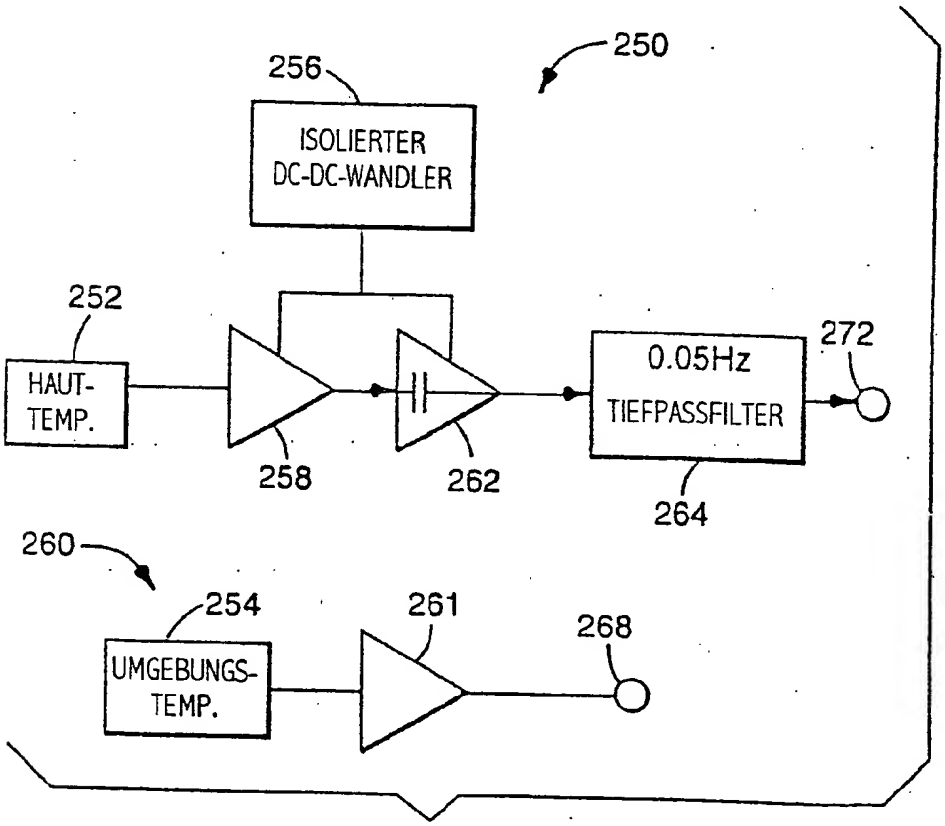
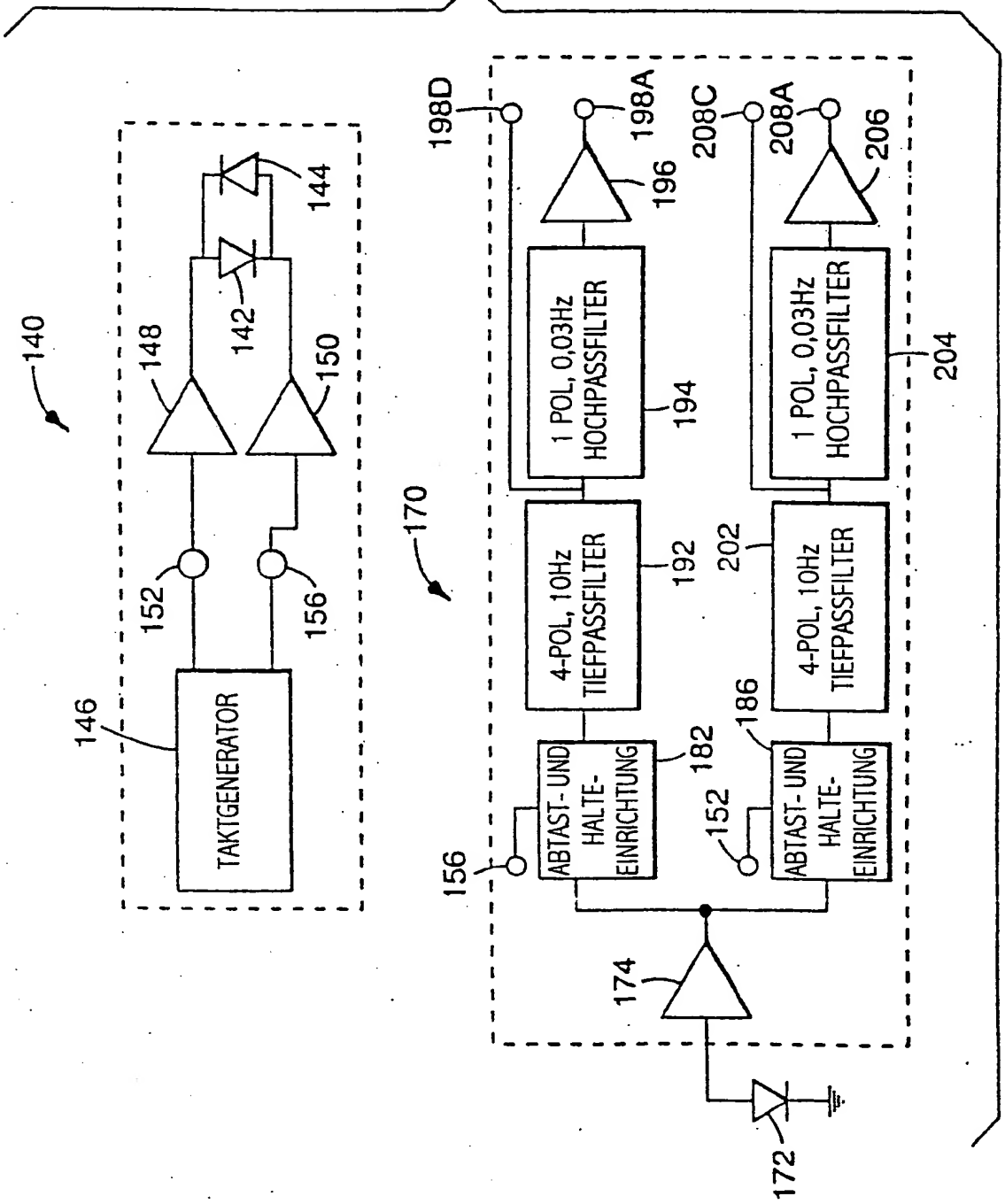

250
256
ISOLIERTER
DC-DC-WANDLER
252
HAUT-
TEMP.
258
262
0.05Hz
TIEFPASSFILTER
264
272
260
254
UMGEBUNGS-
TEMP.
261
268

Fig. 6

Fig. 5


140
148
142
144
150
152
156
146
TAKTGENERATOR
170
198D
198A
196
208C
208A
206
1 POL, 0,03Hz HOCHPASSFILTER
194
204
4-POL, 10Hz TIEFPASSFILTER
192
202
186
182
ABTAST- UND HALTE- EINRICHTUNG
156
152
174
172

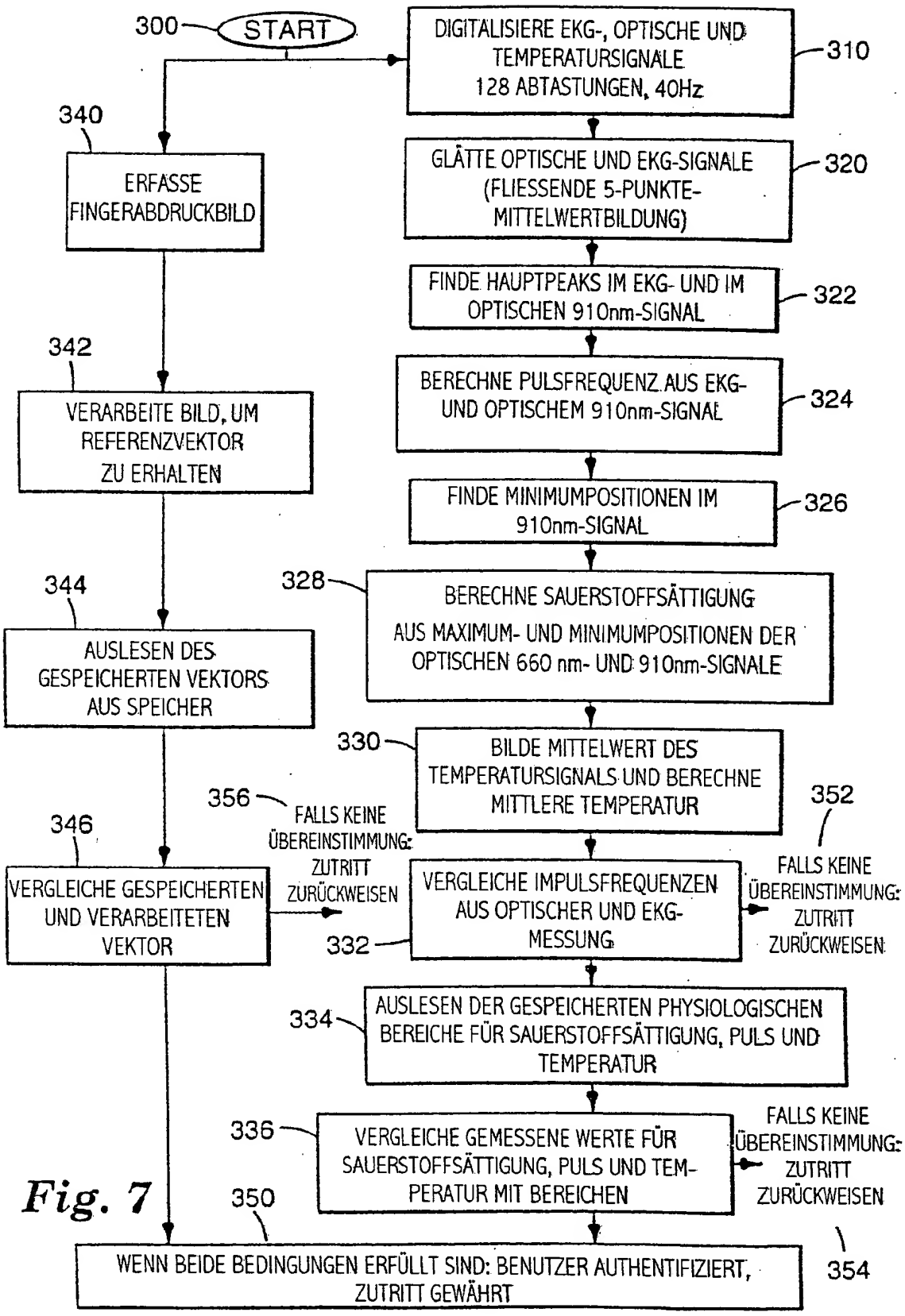

300
START
DIGITALISIERE EKG-, OPTISCHE UND TEMPERATURSIGNALE 128 ABTASTUNGEN, 40Hz
310
340
ERFASSE FINGERABDRUCKBILD
GLÄTTE OPTISCHE UND EKG-SIGNALE (FLIESSENDE 5-PUNKTE-MITTELWERTBILDUNG)
320
FINDE HAUPTPEAKS IM EKG- UND IM OPTISCHEN 910nm-SIGNAL
322
342
VERARBEITE BILD, UM REFERENZVEKTOR ZU ERHALTEN
BERECHNE PULSFREQUENZ AUS EKG- UND OPTISCHEM 910nm-SIGNAL
324
FINDE MINIMUMPOSITIONEN IM 910nm-SIGNAL
326
328
344
AUSLESEN DES GESPEICHERTEN VEKTORS AUS SPEICHER
BERECHNE SAUERSTOFFSÄTTIGUNG AUS MAXIMUM- UND MINIMUMPOSITIONEN DER OPTISCHEN 660 nm- UND 910nm-SIGNALE
330
BILDE MITTELWERT DES TEMPERATURSIGNALS UND BERECHNE MITTLERE TEMPERATUR
356
FALLS KEINE ÜBEREINSTIMMUNG: ZUTRITT ZURÜCKWEISEN
352
346
VERGLEICHE GESPEICHERTEN UND VERARBEITETEN VEKTOR
VERGLEICHE IMPULSFREQUENZEN AUS OPTISCHER UND EKG-MESSUNG
FALLS KEINE ÜBEREINSTIMMUNG: ZUTRITT ZURÜCKWEISEN
332
334
AUSLESEN DER GESPEICHERTEN PHYSIOLOGISCHEN BEREICHE FÜR SAUERSTOFFSÄTTIGUNG, PULS UND TEMPERATUR
336
VERGLEICHE GEMESSENE WERTE FÜR SAUERSTOFFSÄTTIGUNG, PULS UND TEMPERATUR MIT BEREICHEN
FALLS KEINE ÜBEREINSTIMMUNG: ZUTRITT ZURÜCKWEISEN
350
WENN BEIDE BEDINGUNGEN ERFÜLLT SIND: BENUTZER AUTHENTIFIZIERT, ZUTRITT GEWÄHRT
354

Fig. 7

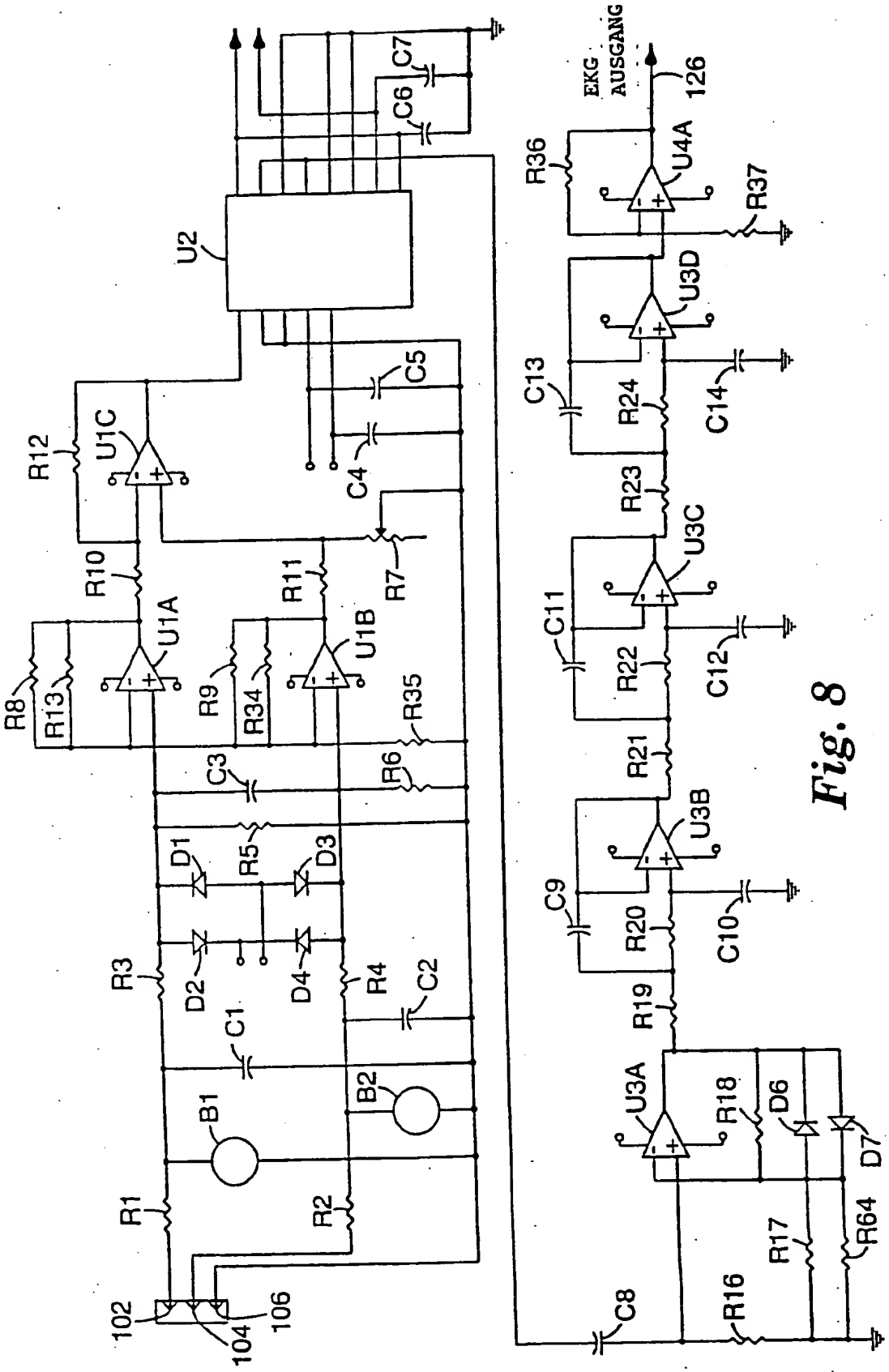

EKG AUSGANG
126
U2
U1A
U1B
U1C
U3A
U3B
U3C
U3D
U4A
R1
R2
R3
R4
R5
R6
R7
R8
R9
R10
R11
R12
R13
R17
R18
R19
R20
R21
R22
R23
R24
R34
R35
R36
R37
R64
C1
C2
C3
C4
C5
C6
C7
C8
C9
C10
C11
C12
C13
C14
D1
D2
D3
D4
D6
D7
B1
B2
102
104
106

Fig. 8

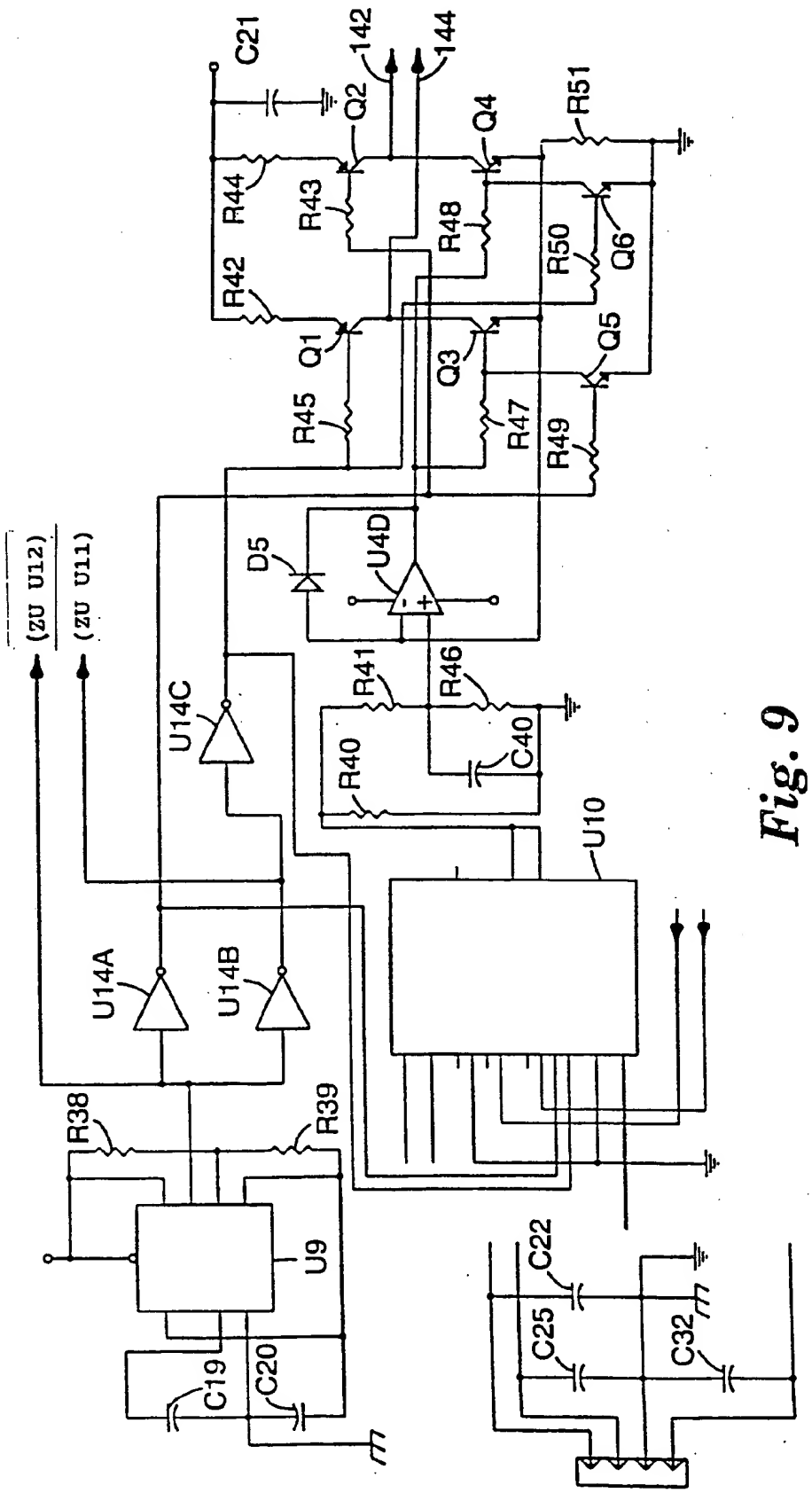

C21
142
144
Q2
Q4
R51
R44
R43
R48
R50
Q6
R42
Q1
Q3
Q5
R45
R47
R49
D5
U4D
(ZU U12)
(ZU U11)
U14C
R41
R46
C40
R40
U10
U14A
U14B
R38
R39
U9
C19
C20
C22
C25
C32

Fig. 9

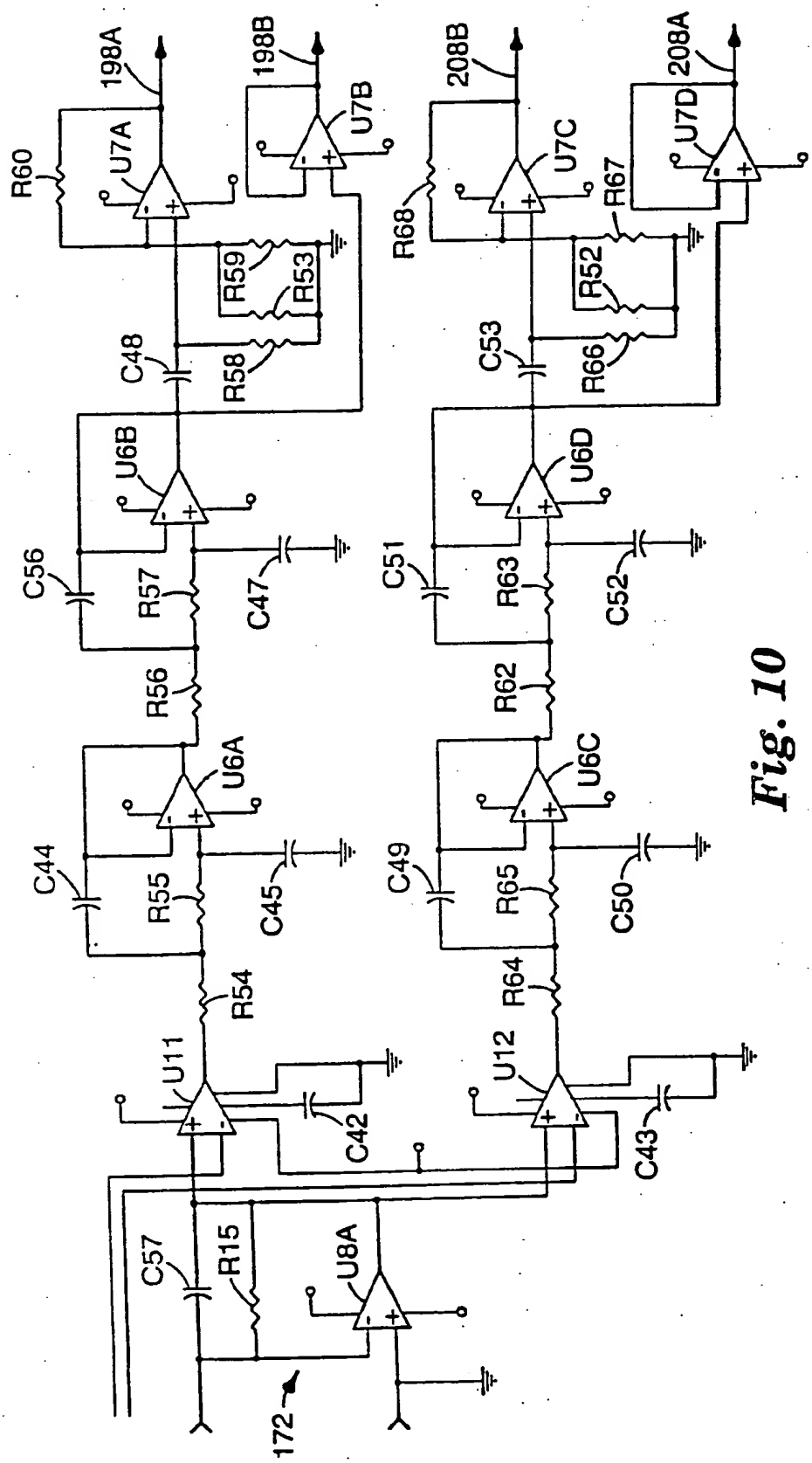

198A
198B
208B
208A
U7A
U7B
U7C
U7D
R60
R68
R67
R59
R53
R52
C48
C53
R58
R66
U6B
U6D
C56
C51
R57
C47
R63
C52
R56
R62
U6A
U6C
C44
C49
R55
C45
R65
C50
R54
R64
U11
U12
C42
C43
C57
R15
U8A
172

Fig. 10

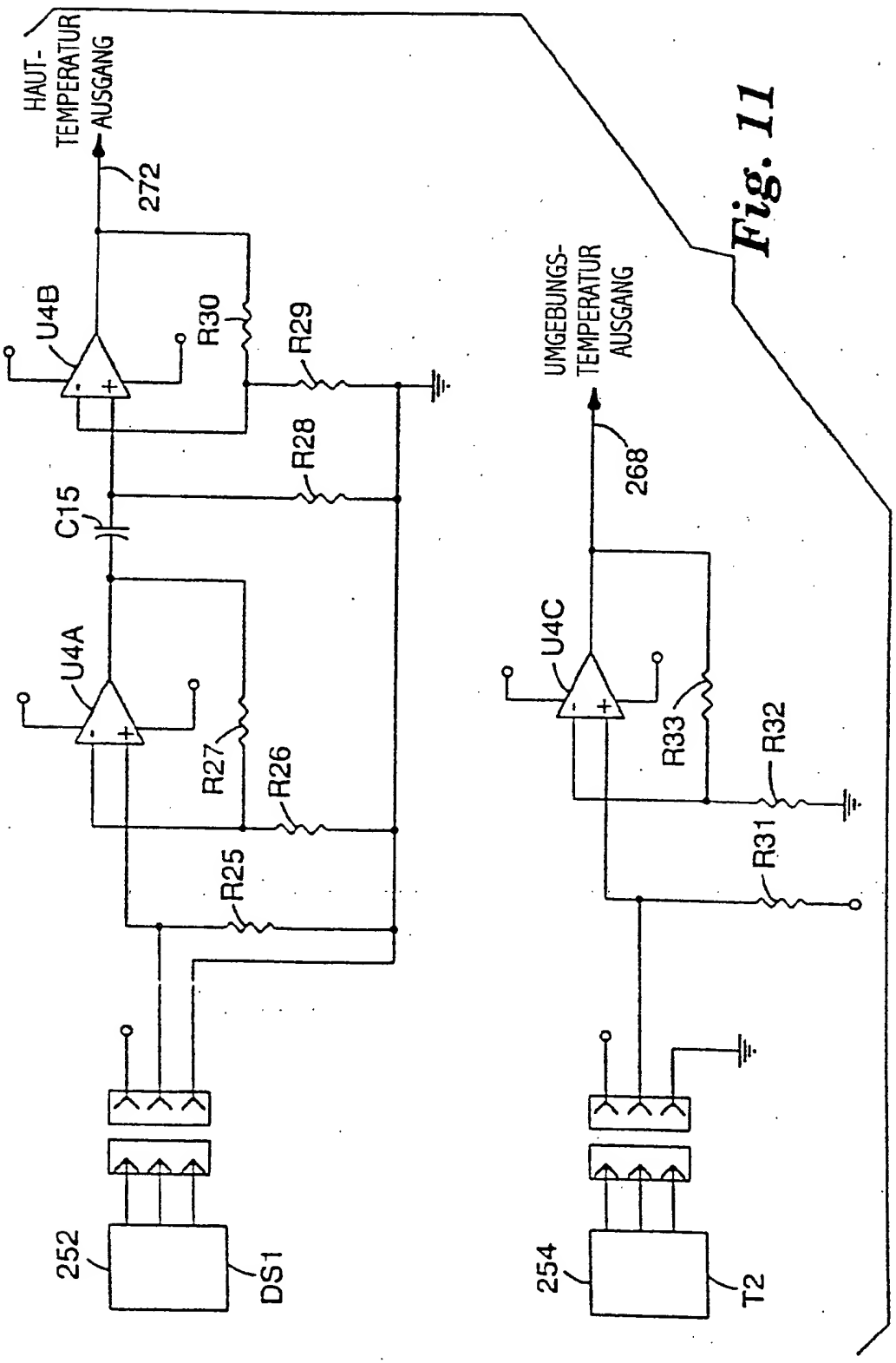

HAUT-
TEMPERATUR
AUSGANG
272
U4B
R30
R29
R28
C15
U4A
R27
R26
R25
252
DS1
UMGEBUNGS-
TEMPERATUR
AUSGANG
268
U4C
R33
R32
R31
254
T2

Fig. 11